implementation agency. Furthermore, the Korea Agency for Defense Development is engaged in the development and use of various satellites.

Section 3 Trends in Cyber Domain

1 Cyberspace and Security

Owing to the advancement of information and communications technology (ICT) in recent years, information and communications networks such as the Internet have become essential components across all facets of life. Therefore, cyber attacks[1] against information and communications networks have the potential to seriously impact the lives of individuals.

Types of cyber attacks include functional disruption, data falsification and data theft caused by unauthorized access to information and communications networks or through the transmission of viruses via e-mail, functional impairment of the networks through simultaneous transmission of large quantities of data, and attacks intended to shut down or take over a system belonging to critical infrastructure, such as power systems. Also, Internet-related technologies are constantly evolving, with cyber attacks becoming more and more advanced and sophisticated by the day.[2]

For military forces, information and communications capability form the foundation of command and control, which extend from central command to ground-level forces. In this regard, ICT advancements are further enhancing the dependence of military forces on information and communications networks. Furthermore, in some cases, military forces need various critical infrastructures, including electricity, to execute their missions. Accordingly, cyber attacks against such critical infrastructures could become a major impediment to their missions. For this reason, cyber attacks are recognized as an asymmetrical means to impede the military activities of adversaries at low cost. It is believed that many foreign military forces are developing offensive capabilities in cyberspace. It has been pointed out that China and Russia in particular are bolstering the offensive cyber capabilities of their militaries for the purpose of obstructing the networking of military forces and destroying infrastructure.[3]

In addition, actors (including non-state actors) attempting to cause harm to nations, etc. are likely to realize that attacking through cyberspace is often easier than attacking directly by physical means.[4] Moreover, it is said that the information and communications networks of countries are being compromised for the purpose of gathering intelligence. As more confidential information is stored in cyberspace, information theft through cyber attacks is causing more serious damage.

2 Threats in Cyberspace

Under such circumstances, cyber attacks have frequently been carried out against information and communications networks of government organizations and military forces of various countries.[5] Government agencies are suspected of engaging in some cyber attacks. Military forces in China, Russia, and North Korea are believed to be enhancing their cyber attack capabilities.

1 The targets of cyber attacks are wide-ranging. Beginning with large targets, they range from global-level targets, including inter-state targets, as well as national and government institutions, local communities, business communities and, infrastructures, companies, and individuals. As such, it is said that measures to counter cyber attacks need to be optimal relative to the size of the target.

2 In the Japanese Ministry of Defense (MOD)'s "Toward Stable and Effective Use of Cyberspace" of September 2012, cyber attacks are characterized as follows: (1) diversity: cyber attacks involve diverse actors, methods, objectives, and context; (2) anonymity: actors can easily conceal and disguise their identity; (3) stealth: some cyber attacks are difficult to identify and can take place without causing any realization of damage; (4) offensive dominance: attack tools are easy to acquire depending on the tool, and it is difficult to completely eliminate software vulnerabilities; and (5) the difficulties of deterrence: retaliatory strikes and defensive measures have minimal deterrence effect.

3 According to the "Worldwide Threat Assessment" by the Director of the U.S. Defense Intelligence Agency (March 2018).

4 According to the "Cybersecurity National Action Plan" unveiled by then U.S. President Obama in February 2016.

5 According to the annual report presented to Congress by the U.S. Office of Management and Budget based on the Federal Information Security Management Act, the number of cybersecurity incidents reported to federal offices in FY2017 in the U.S. was 35,277. Moreover, the "Worldwide Threat Assessment" of January 2019 by the U.S. Director of National Intelligence names China, Russia, Iran, and North Korea as those that pose the greatest cyber threats to the United States. It also indicates (1) that China presents a persistent cyber espionage threat and a growing attack threat to U.S. core military and critical infrastructure systems, (2) that Russia poses a cyber espionage, influence, and attack threat to the United States and its allies, (3) that Iran presents a cyber espionage and attack threat, and (4) that North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks.

1 China

According to China's defense white paper called "China's Military Strategy" (May 2015),[6] China will expedite the development of a cyber force. Furthermore, it has been pointed out that cyber warfare units have been formed under the Strategic Support Force that was created as part of China's military reforms[7] in late December 2015. The units are estimated to consist of 175,000 troops, including 30,000 for cyber attacks, indicating that China is enhancing its military's cyber warfare capabilities.

China is suspected of conducting cyber attacks to steal confidential information even in peacetime.[8] For example, its involvement in the following incidents has been pointed out.

- In June 2015, the U.S. Office of Personnel Management (OPM) became a target of a cyber attack in which, as it later came to light, personal information of about 22 million people, including U.S. federal employees and U.S. Forces personnel, were stolen.[9]
- In January and February 2018, Chinese government hackers hacked a U.S. Navy contractor, leading to a leak of classified information on supersonic anti-ship missiles mounted on submarines.[10]
- In December 2018, such countries as the United States announced that the APT10 cyber group related to China's Ministry of National Security conducted cyber attacks on intellectual and other properties in at least 12 countries. The United States pointed out that the APT10 group implemented cyber attacks on government agencies of these countries and stole defense, space, aviation, resources development, and other information from U.S. companies.

Even in Japan, it has been confirmed that the APT10 group conducted extensive cyber attacks on private enterprises, academic organizations and other targets over a long term.

2 Russia

It has been revealed that the Russian military has its own cyber commando unit, which is believed to be responsible for conducting offensive cyber activities,[11] including inserting malware into command and control systems of adversaries.[12]

It is pointed out that Russia has taken advantage of cyberspace for intelligence operations to challenge democratic processes,[13] and has been involved in the following incidents.

- In 2014, more than 500 million user accounts were leaked from a major U.S. Internet company. In March 2017, the U.S. government indicted four hackers, including two officers of the Russian Federal Security Service (FSB), for their alleged cyber attack on the company.[14]
- In December 2015, a cyber attack triggered a large-scale power outage in Ukraine. It was reported that military forces of Russia confronting with Ukraine over the Crimea annexation and other issues were suspected of having contributed to the cyber attack.
- Cyber attacks to affect the outcome of the 2016 U.S. presidential election.[15]
- In June 2017, cyber attacks using the so-called NotPetya ransomware occurred in Ukraine and other countries. In February 2018, the U.S. and U.K. governments attributed the attacks to the Russian military.
- In October 2018, the U.S. and U.K. governments announced that the Main Intelligence Directorate of the General Staff of the Russian Armed Forces was responsible for cyber attacks on the World Anti-Doping Agency, the

6 The defense white paper notes that "cyberspace has become a new pillar of economic and social development, and a new domain of national security," that "as international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces," and that China is "one of the major victims of hacker attacks."

7 While the details of the Strategic Support Force's tasks and organization have not been revealed, it is suggested that it is in charge of outer space, cyber, and electronic warfare. See Part I, Chapter 2, Section 2 regarding the Strategic Support Force.

8 According to the DoD Cyber Strategy released in September 2018, Chinese cyber attacks involve a range of organizations, including the People's Liberation Army (PLA), intelligence agencies, security agencies, private hacker groups, and companies. The Annual Report of the U.S.-China Economic and Security Review Commission (November 2016) notes that China carries out cyber espionage led by the Ministry of State Security and military organizations as well as cyber espionage led by China's many non-state actors targeting the United States. These actors include hackers contracted by the government, civilian "patriotic hackers," and criminal organizations.

9 See the Annual Report of the U.S.-China Economic and Security Review Commission (November 2015). In addition to this attack, the report states that a U.S. airline company was attacked by the same method as that used in the attack against the U.S. OPM.

10 The United States deems that China continues to conduct cyber-enabled theft targeting a broad set of U.S. interests ranging from national security information to sensitive economic information and U.S. intellectual property. While the United States and China have agreed to refrain from cyberespionage of intellectual property, it has been pointed out that cyber espionage by China still continues unimpeded.

11 According to a statement made by Russian Minister of Defence Shoigu during a briefing for the lower house in February 2017, the Russian military has a cyber command for the defensive purpose of countering political propaganda in Russia's ongoing information war with Western countries. It is pointed out that the number of Russia's cyber troops comes to approximately 1,000.

12 According to then U.S. Director of National Intelligence Clapper's written testimony on "Worldwide Cyber Threats" at the House Permanent Select Committee on Intelligence in September 2015.

13 According to the "DoD Cyber Strategy" released in September 2018.

14 There was another cyber attack on this Internet company in 2013, resulting in the leaking of information on approximately 3 billion people.

15 According to the joint statement issued in October 2016 by the U.S. Department of Homeland Security and the director of National Intelligence of the United States, and the joint report issued in December of the same year by the U.S. Department of Homeland Security and the FBI concerning Russian cyber attacks on the United States, as well as the U.S. intelligence community report on Russia's cyber attacks on the U.S. presidential election released in January 2017. Moreover, during the 2017 presidential campaign in France, Macron, known as a hardliner on Russia, was reportedly a target of a cyber attack, as well as a widespread fake news story about having hidden assets in a tax haven. After being appointed president, in a joint press conference of the French and Russian presidents, Macron criticized Russian media outlets by name, referring to them as organs of lying propaganda.

Organization for the Prohibition of Chemical Weapons, the U.S. Democratic convention, and other targets.

3 North Korea

It has been pointed out that the North Korean authority trains hackers [16] and has intensively built up cyber units operating some 6,800 personnel.[17]

North Korea is believed to have been developing capabilities to steal money and secret military information through cyber attacks and inflict such attacks on key foreign infrastructure. It is suspected of having been involved in the following incidents.

- In September 2016, cyber attacks occurred in the internal network of the ROK Armed Forces. In May 2017, the ROK Ministry of National Defense was reported to have concluded that the cyber attacks had been conducted by what was believed to be a North Korean hacker group.[18] Moreover, it has been pointed out that documents containing military secrets were stolen through the cyber attacks.
- In May 2017, a cyber attack used a malware called WannaCry to encrypt and neutralize electronic data held by hospitals, schools, businesses, and other entities in more than 150 countries. The Japanese, U.S., and U.K. governments blamed North Korea for the attack.[19] It has been pointed out that this cyber attack succeeded in collecting 140,000 dollars in Bitcoins.
- In September 2017, multiple U.S. electric power utilities were inflicted with cyber attacks using spear phishing emails. In October 2017, FireEye, a U.S. cybersecurity company, announced that the attacks had been conducted by a cyber threat group allegedly affiliated with North Korea.
- In February 2018, according to the ROK National Intelligence Service, North Korea has repeatedly hacked the ROK exchanges for the purpose of stealing virtual currencies, and it has succeeded in acquiring the equivalent of several dozen billion won (several billion yen).
- In March 2019, a final report by an expert panel of the United Nations Security Council's North Korea Sanctions Committee pointed out that North Korea conducted at least five cyber attacks on virtual currency exchanges in Japan and other Asian countries between January 2017 and September 2018, stealing a total of 571 million dollars (about 63 billion yen).

4 Trends Concerning Other Threats

Supply chain risks, including products embedded with deliberately and fraudulently altered programs, and the existence of advanced malware designed to attack industrial control systems are also pointed out. In this respect, the U.S. Congress in August 2018 passed the National Defense Authorization Act of 2019 including provisions prohibiting government agencies from using products of major Chinese communications equipment manufacturers, such as Huawei Technologies Co. The United States has provided its allies with information about risks accompanying Chinese communications equipment and urged them not to use such equipment. In response, Australia has banned China's Huawei and ZTE Corporation from taking part in its 5G next-generation mobile network development project.

Cyber attacks on telecommunication networks of a government and military forces or on critical infrastructure could have a serious effect on the security of states, and it is believed that state-sponsored cyber attacks have been on the rise in recent years. Given this situation, there is a need for continuous monitoring of trends in the threats in cyberspace.

3 Initiatives against Cyber Attacks

Given these growing threats in cyberspace, various initiatives are under way.[20]

A number of issues have been raised that need to be dealt with to enable an effective response to be taken to cyber attacks. It is regarded that the international community has diverging views concerning the fundamental matters of

16 According to the "2016 Defense White Paper" published by the ROK in January 2017, it is said that North Korean cyber-related organizations are linked to the authority, and spot talented human resources from all over the land, giving them special training to develop cyber forces.

17 According to the "2018 Defense White Paper" published by the ROK in January 2019. In November 2013, it was reported that Kim Jong-un, then First Secretary of the Korean Workers' Party of North Korea, stated, "Cyber attacks are omnipotent swords with their power paralleled with nuclear power and missiles."

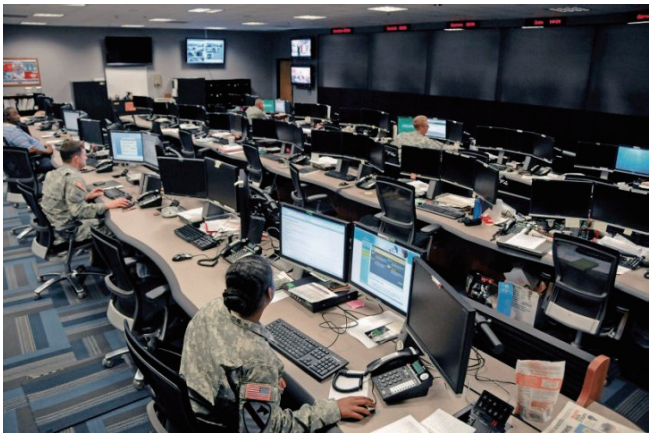
18 According to the digital ROK National Defense Report in May 2017. Furthermore, the report revealed that some of the IP addresses (Internet addresses) used in the attacks were identified as those in the Shenyang region of China, known to have been used by existing North Korean hackers.

19 Japan, the United States, the United Kingdom, Australia, Canada, and New Zealand issued a statement of condemnation. Moreover, according to JPCERT/CC, over 2,000 devices at 600 locations in Japan are said to have been infected.

20 Generally, the trends at the governmental level are thought to include the following: (1) organizations related to cybersecurity that are spread over multiple departments and agencies are being integrated, and their operational units are being centralized; (2) policy and research units are being enhanced by establishing specialized posts, creating new research divisions and enhancing such functions; (3) the roles of intelligence agencies in responding to cyber attacks are being expanded; and (4) more emphasis is being given to international cooperation. At the level of the defense ministry, various measures have been taken, such as establishing a new agency to supervise cyberspace military operations and positioning the effort to deal with cyber attacks as an important strategic objective.

cyberspace, including how international law applies. For instance, the United States, Europe, and Japan have called for maintaining a free cyberspace, while Russia, China, and most emerging countries sought to strengthen state control on cyberspace. Against this backdrop, there has been a movement to promote the rule of law in cyberspace in the international community. For instance, discussions are being held on the establishment of international rules within the framework of global conferences on cyberspace.[21]

See Part III, Chapter 1, Section 2-3-2 (Response in Cyber Domain)



U.S. Army Cyber Command
[Jane's by IHS Markit]

1 The United States

In the United States, the Department of Homeland Security is responsible for protecting Federal government networks and critical infrastructure against cyber attacks, and the Department's Office of Cybersecurity and Communications (CS&C) works to protect the networks of government agencies.[22]

The U.S. National Security Strategy (December 2017) points out that many countries now view cyber capabilities as tools for projecting influence and that cyberattacks have become a key feature of modern conflict. It also notes that the United States would deter, defend, and when necessary defeat malicious actors who inflict cyber attacks on the United States. To this end, the U.S. strategy came up with policy (1) to improve ability to attribute cyberattacks and allow for rapid response, (2) to enhance cyber tools and expertise to protect U.S. government assets, critical infrastructure, and information, and (3) to improve the integration of authorities and procedures across the U.S. government so that cyber operations against adversaries can be conducted as required. The U.S. DoD in its National Defense Strategy (January 2018) described a policy of investing in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Furthermore, the DoD Cyber Strategy (September 2018) points out that the United States is engaged in a long-term strategic competition with China and Russia, and that China and Russia have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the United States as well as to its allies and partners.[23] The strategy presents such approaches as (1) the acceleration of cyber capability development, (2) defense to counter and deter malicious cyber activity, and (3) the promotion of cooperation with U.S. allies and partners. In April 2019, U.S.-Japan Security Consultative Committee (two-plus-two) convened, where the two countries agreed to enhance cooperation on cyber issues and affirmed that international law applies in cyberspace and that a cyber attack could, in certain circumstances, constitute an armed attack for the purposes of the U.S.-Japan Security Treaty.

The U.S. Forces include Cyber Command, which was elevated to a unified combatant command in May 2018, to control cyberspace operations. The Command consists of the Cyber Protection Force, which operates and protects the information infrastructure for the cyber forces of the U.S. Army, Navy, Air Force, and Marine Corps and for the DoD, the National Mission Force, which supports U.S. defense against national-level threats, and the Combat Mission Force, which supports the operations conducted by unified combatant commands on the cyber front (these three forces are collectively referred to as the Cyber Mission Force[24]).[25]

2 North Atlantic Treaty Organization (NATO)

NATO Policy on Cyber Defence, and its action plan, which

21 Global conferences on cyberspace have been held since being proposed by the then U.K. Foreign Secretary Hague in 2011, and the series of conferences has been called the "London Process." The conferences have been attended by the governments, international organizations, groups from the private sector, NGOs, etc., of over 100 countries, and comprehensive discussions are held on various issues regarding cyberspace. They are high-level, large-scale global conferences, and the most recent one was held in November 2017.

22 The U.S. Department of Homeland Security announced a cybersecurity strategy in May 2018. More than 20 billion devices are expected to become connected to the Internet by 2020, and this is also said to increase the risks.

23 The DoD Cyber Strategy indicated a view that, while China is eroding U.S. military overmatch and economic vitality by exfiltrating sensitive information from U.S. public and private sector institutions, Russia has used cyber-enabled information operations to influence the U.S. population and challenge U.S. democratic processes.

24 According to the DoD, the Cyber Mission Force has 133 teams (13 National Mission Teams, 68 Cyber Protection Teams, 27 Combat Mission Teams and 25 Support Teams), comprising 6,200 persons.

25 U.S. Cyber Command, which had been subordinate to U.S. Strategic Command, was elevated to a unified combatant command in May 2018, allowing the CYBERCOM commander to report directly to the U.S. Secretary of Defense as is the case with other unified combatant command commanders. In announcing the elevation of U.S. Cyber Command to a combatant command, the U.S. DoD has stated that the domain of cyberspace is just as important for military operations as land, sea, and air, and that operational capabilities in cyberspace are indispensable for military success. The DoD indicated that the future issues will be the bolstering of cyber weapons, cyber defense, and the scale and capabilities of cyber personnel.

were adopted in June 2011: (1) clarify the political and operational mechanisms of NATO's response to cyber attacks; (2) clarify that NATO would provide assistance to member states to develop their cyber defense, and provide assistance to member states if they are subject to cyber attacks; and (3) set out principles on cooperation with partners. Furthermore, at the NATO Summit in September 2014, agreement was reached that NATO's collective defense applies to cyber attacks against member states.

On the organizational front, in November 2017, an agreement was reached on the creation of a new Cyber Operations Center and the integration of NATO member countries' cyber defense capabilities into NATO missions and operations. The Cyber Operations Center located in Belgium is expected to be fully operational with cyber attack capabilities by 2023. Furthermore, NATO has conducted cyber defense training exercises annually since 2008 to heighten cyber defense capabilities. In addition, NATO has expanded cooperation with the EU in the fields of cybersecurity and cyber defense.[26]

In 2008, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was authorized to serve as a research and training institution,[27] and was established in Estonia's capital of Tallinn. CCDCOE carries out research on the relationship between cyber activities and international law, creating the "Tallinn Manual."[28] In February 2017, "Tallinn Manual 2.0" was published as the second edition of the previous manual based on a review of broad discussion points, from peacetime legal regimes, such as laws on state responsibility, human rights, aviation, space, and maritime affairs, to contingency legal regimes, such as laws on armed conflict.

3 The United Kingdom

The United Kingdom, in its "NSS- SDSR2015" released in November 2015, committed to investing £1.9 billion over the next five years in increasing its cyber defense capabilities to strengthen the functions for identifying and analyzing cyberspace threats. In November 2016, the country announced a new "Cyber Security Strategy" that presents a vision for the United Kingdom, which is to be secure and resilient to cyber threats, prosperous and confident in the digital world. To achieve this vision, the Strategy requires the United Kingdom to deter cyber threats by having effective defensive and offensive means and to "develop" cutting-edge technologies.

On the organizational front, in October 2016, the National Cyber Security Centre (NCSC) was newly established under the Government Communications Headquarters (GCHQ) to promote public-private partnerships for responses to national cyber incidents.

4 Australia

In its first "National Security Strategy" published in January 2013, Australia positions integrated cyber policies and operations as one of the top national security priorities. In April 2016, a new "Cyber Security Strategy" through 2020 was released, which provides that Australia will ensure the safety of the people, that private companies will participate in cybersecurity, and that threat information will be shared.

On the organizational front, cybersecurity capabilities across the government were converged to establish the Australian Cyber Security Center (ACSC), which addresses major cybersecurity issues related to government agencies and critical infrastructures.[29] In July 2015, the ACSC issued its first report on cybersecurity,[30] which contends that the number, type, and sophistication of cyber threats to Australia are all increasing. Moreover, cyber forces were established within the military in July 2017 to strengthen the Department of Defence's cyber capabilities and systems.[31]

5 The ROK

The ROK formulated the "National Cyber Security Master Plan" in August 2011, which clarifies the supervisory functions of the National Intelligence Service[32] in responding

26 In July 2016, NATO and the EU signed a Joint Declaration with the aim of expanding cooperation in dealing with new issues, such as those involving terrorism, refugees and immigrants, including the cybersecurity issues. They have been strengthening cooperation, for example, by exchanging information on cyber defense.

27 In June 2013, the NATO Defense Ministers' Meeting placed cyber attacks at the top of the agenda for the first time. They agreed to establish an emergency response team and to implement a cyber defense mechanism on a full scale by October 2013.

28 The "Tallinn Manual" and the "Tallinn Manual 2.0" are both considered independent outputs of the members that participated in the project (Professor Michael N. Schmitt of the U.S. Naval War College served as project leader; members included professionals, scholars on international law, and experts in cyber technology in the West and other areas), and not the official view of NATO.

29 The ACSC, comprised of staff from the Australian Crime Commission, the Australian Federal Police, the Australian Security Intelligence Organisation, the Australian Signals Directorate, and the Australian Federal Computer Emergency Response Team, and the Defence Intelligence Organisation, analyzes cyber threats and responds incidents in both private and public sector.

30 According to the report, malicious actors in cyberspace targeting Australia are: (1) foreign government-sponsored adversaries; (2) serious and organized criminals; and (3) groups motivated by certain issues and individuals with personal grievances.

31 According to "International Cyber Engagement Strategy" announced in October 2017, the country's offensive cyber capability in support of military operations will be deployed through the Signals Directorate in cooperation with the Australian Force.

32 Under the Director of the National Intelligence Service, the National Cybersecurity Strategy Council has been established to deliberate on important issues, including establishing and improving a national cybersecurity structure, coordinating related policies and roles among institutions, and deliberating measures and policies related to presidential orders.

to cyber attacks. It places particular emphasis on strengthening the following five areas: prevention, detection, response,[33] systems, and security base. In the national defense sector, the Cyber Measures Technology Team was established by the Ministry of National Defense to respond to cyber and hacking threats. The sector has also worked out procedures for quick response to cyber crises under the "National Cyber Security Strategy" and the "National Cybersecurity Crisis Response Manual." In 2015, the Joint Chiefs of Staff centralized the cyber attack tactical system mainly around the Joint Chiefs of Staff by newly establishing the Cyber Tactics Department, assigning control authority concerning cyber tactics to the Chairman of the Joint Chiefs of Staff, and issuing a field manual on "joint cyber tactics."

33 In February 2014, the ROK Ministry of National Defense reportedly briefed the National Assembly that it planned to develop cyber weapons for attacking other countries.